



National Infrastructure Protection Center CyberNotes

Issue #13-99

June 21, 1999

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 7 and June 18 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
America on Line ¹	AOL Instant Manager (AIM) 2.0	In the newest version of AIM (AOL Instant Messenger) security hole exists that allows remote attacker to get user IP address.	No workarounds or patches known at time of publishing	IP Address Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Apple ²	MacOS X Server	MacOS X Server running Apache crashes when 32 or more processes are doing GET requests to a Common Gateway Interface (CGI) script. Every web site operating under MacOS X Server can be paralyzed.	No patch available at time of publishing. Workaround: Deactivate the execution of CGI scripts.	CGI Script Exploit	Low	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability appears in the press.

¹ Bugtraq, June 8, 1999.

² Bugtraq, June 3, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco Gigabit Switch Routers (12008 and 12012 GSRs) ³	IOS Software 11.2(14) GS2 through 11.2(15) GS3	Unauthorized access to systems and release of information can be obtained due to an error encountered while processing the established keyword in an access-list statement. Unauthorized traffic can be forwarded.	Upgrade to Release 11.2(15)GS5 and later versions (Cisco is offering free software upgrades)	Access List Keyword Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploiting the flaw requires no special tools or knowledge.
Compac ⁴	Tru64/Digital Unix V4.0bm V4.odm V4.oem V4.Of 0e, Of	Potential vulnerability exists with the /usr/dt/bin/dtlogin where under certain circumstances, a user may gain unauthorized access as superuser.	Apply the vendor-supplied patch located at: http://www.service.digital.com/patches Use the FTP access option, select DIGITAL_UNIX directory, then choose the appropriate version directory and download the patch accordingly.	Dtlogin Security Vulnerability	High	Bug discussed in newsgroups and websites.
Hewlett-Packard ⁵	OmniHTTPd Web Servers	Temporary files on the server can be made (remotely) until server's HDD is full which results in a Denial of Service attack.	Fix: Remove visadmin.exe from cgi-bin directory.	Server HDD Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard ⁶	HP9000 Series 700/800	Netscape Enterprise Server (NES) fails to properly process some URLs. This activity has been observed in the NES bundled with Praesidium VirtualVault Release A.02.00, A.03.00, A.03.01 & A.03.50.	Apply the appropriate patches: A.02.00 US/Canada/Int'l: PHCO_18615 PHSS_18620 A.03.00 US/Canada/Int'l: PHCO_18615 PHSS_18616 A.03.01 US/Canada/Int'l: PHCO_18615 PHSS_18612 A.03.50 US/Canada/Int'l: PHCO_18615 PHSS_18621	VVOS NES Vulnerability	Low	Bug discussed in newsgroups and websites.
Internet Software Consortium ⁷	Red Hat Linux 6.0 (all architectures)	Flaw in the way RedHat displays remote TTY's can be exploited to cause disruption to anyone using X-Windows on the local machine, which results in a Denial of Service attack.	Upgrade to the latest errata releases of dev, screen and rxvt for Red Hat Linux 6.0 on your particular platform. You will have to manually unmount and remount the /dev/pts file system with the following commands, once the correct permissions have been set in the /etc/fstab file: umount /dev/pts mount /dev/pts	Permissions Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

³ Cisco Security Bulletin, June 10, 1999.

⁴ CIAC Bulletin, June 1, 1999.

⁵ Bugtraq, June 5, 1999.

⁶ Hewlett-Packard Company Security Bulletin: #00098, June 10, 1999.

⁷ Bugtraq, June 6, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Internet Software Consortium ⁸	Red Hat Linux 6.0 (Sparc version only)	This bug allows a Denial of Service attack against programs utilizing the ORBit CORBA implementation, which causes these programs to crash.	Upgrade to: rpm -Uvh ORBit-0.4.3- 3.sparc.rpm rpm -Uvh ORBit-devel.0.4.3- 3.sparc.rpm Those planning to recompile ORBit should upgrade their tcp_wrappers to the tcp_wrappers-7.6-8.sparc.rpm package.	ORBit /tcp_wrappers Vulnerability	Low	Bug discussed in newsgroups and websites.
Internet Software Consortium ⁹	Red Hat Linux	This is a maintenance release of the wu-ftpd package that corrects problems with file name globbing that were broken in a previous errata. All known exploits fixed on all current Red Hat releases.	Solution: <u>Intel</u> : Upgrade to: rpm -Uvh wu-ftpd-2.5.0-2.i386.rpm <u>SPARC</u> : Upgrade to: rpm - Uvh wu-ftpd-2.5.0-2.sparc.rpm <u>Alpha</u> : Upgrade to: rpm -Uvh wu-ftpd-2.5.0-2.alpha.rpm <u>Source</u> : rpm -Uvh wu-ftpd- 2.5.0-2.src.rpm	File Name Globbing Vulnerability	Low	
Internet Software Consortium ¹⁰	Red Hat Linux 6.0 PAM-enabled machines	When you try to su to root if it's successful, immediately gives you a shell prompt. Otherwise, it delays a full second, then logs an authentication failure to syslog. If you hit break in that second, no error, plus you know that the password was bad, so you can brute force root's password.	No workaround or patch at time of publishing.	Root Password Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Solaris 2.5 and below ¹¹	Solaris /bin/su on 2.5	The same vulnerability as the Red Hat Linux 6.0 Pam-enabled machines which is described above.	Upgrade to Solaris 2.6	Root Password Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

⁸ Red Hat Security Advisory, June 6, 1999.

⁹ Red Hat Security Advisory, June 10, 1999.

¹⁰ Bugtraq, June 9, 1999.

¹¹ Bugtraq, June 10, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun ^{12, 13, 14}	SunOS 5.3-5.6; SGI IRIX 5.3	The vulnerability in rpc.statd allows an intruder to call arbitrary rpc services with the privileges of the rpc.statd process. The vulnerability in automountd allows a local intruder to execute arbitrary commands with the privileges of the automountd process. By exploiting these two vulnerabilities simultaneously, a remote intruder is able to "bounce" rpc calls from the rpc.statd service to the automountd serviced on the same targeted machine.	Patches for Sun customers available at: http://sunsolve.sun.com/pub/cgi/show.pl?target=patches/patch-license&nav=pub-patches SunOS 4.1.3 & 4.1.4 are still vulnerable to the rpc.statd bounce attack with no patches currently releases. IRIX 6.2 & above are not vulnerable. IRIX 5.3 is vulnerable, but no longer supported; automountd with patches from SGI Security Advisory 19981005-01-PX installed.	Rpc.statd & Automountd Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE ¹⁵	Debian GNU/Linux 2.1	The man-db package has a vulnerability in the Zsoelim program that makes it vulnerable to a symlink attack	Upgrade your man-db package to version 2.3.10-69GIX.1	Symlink Attack Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE ¹⁶	Linux 6.1	In the shadow-980724 package, the 'useradd' command has an option '-p password' for specifying password to the newly added user. If you specify this option along with a password, the password will be stored in /etc/shadow, but in cleartext.	Upgrade to the current version (19990607) available at: ftp://piast.t19.ds.pwr.wroc.pl/pub/linux/shadow/	Cleartext Password Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
SuSE ¹⁷	Linux 6.1	In the shadow 1990307 package, a new user is created with UID 65536; he will become root upon login. No root login will be logged and even if the tty isn't in /etc/securetty he will be allowed in.	No workaround or patch at time of publishing.	UID 65536 and Shadow 1990307 Vulnerability	High	

¹² Sun Security Bulletin #00186, June 7, 1999.

¹³ CERT Advisory CA-99-05, June 9, 1999.

¹⁴ CIAC Bulletin J-045, June 10, 1999.

¹⁵ Bugtraq, June 5, 1999.

¹⁶ Bugtraq, June 11, 1999.

¹⁷ Bugtraq, May 24, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix ¹⁸	KDE's K-Mail 1.1	When K-Mail receives an e-mail with attachments, it creates a directory to store the attachments. K-Mail does not verify that the directory already exists and will to follow symbolic links, allowing local attackers to create files with the contents they choose in any directory writable by the user executing K-Mail. If K-Mail is run as root, unauthorized superuser access may be obtained.	Patch available at: ftp://ftp.kde.org/pub/kde/security_patches/kmail-security-patch.diff	K-Mail File Creation Vulnerability	High	Bug discussed in newsgroups and websites.
Windows 9.x/NT ¹⁹	Microsoft Internet Explorer 5.0	HTML Applications (HTAs) are fully trusted and have read/write access to the system registry, can run embedded ActiveX controls and Java applets, and zone security is off. All operations subject to security zone options are permitted, which opens up a wide range of security holes.	No workarounds or patches known at time of publishing.	HTML Applications Security Hole	High	Bug discussed in newsgroups and websites.
Windows NT ²⁰	Microsoft Windows 2000 (beta release)	FTP PASV vulnerability that allows malicious attacker to hijack your connection and steal the files you attempt to download.	No workarounds or patches known at time of publishing.	Microsoft Win2K PASV Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Windows NT ²¹	Microsoft IIS 2.0 + 3.0 + 4.0	NT 4 Server w/ IIS bug allows any Internet user (IUSR_COMPUTER) to change any user's password, including the administrators, leading to total server compromise	No workarounds or patches known at time of publishing.	Password Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Windows NT ²²	Windows Terminal Server 4.0	The bug occurs when a thread changes its priority. NT changes the thread's priority, but also gives it a new execution quantum. By repeating this process, a single thread can monopolize a CPU.	No workaround or patch available at time of publishing.	Never Ending Quantum Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

¹⁸ ISS Security Advisory, June 9, 1999.

¹⁹ NTBugtraq, June 8, 1999.

²⁰ Bugtraq, June 16, 1999.

²¹ Net Security, June 11, 1999.

²² Bugtraq, June 9, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Windows NT 4.0, 95, 98 ²³	NFS	Character set that can be used in naming files isn't limited by the NFS protocol. Although you cannot create a local file whose name is PRN, you can, however, jump onto a networked server and create (in any directory that you have creatable permissions) any file or directory named PRN.xxx (again, xxx stands for any extension). The directory you've just created is non-removable for as long as it possesses that name.	Workaround: http://support.microsoft.com/support/kb/articles/Q120/7/16.asp	Networked PRN Vulnerability	Low	Bug discussed in newsgroups and websites.
Windows NT, NetWare ²⁴	Fasttrack 3.x	Allows remote attacker to climb the directory tree and view root (and other) directory listings.	Workaround: Disable directory listing.	Unauthorized Directory Listing Vulnerability	Medium	Bug discussed in newsgroups and websites.
Windows NT4 ²⁵ Almost 90% of the Windows NT web servers on the Internet are affected by this hole	Microsoft Internet Information Server 4.0 Microsoft Windows NT 4.0 SP3 Option Pack 4; SP4 Option Pack 4; SP5 Option Pack 4	Allows remote users to gain control by creating a buffer overflow on .httr webpages (a feature designed to enable users to remotely change their password). The break-in code works on any server from which a web page can be retrieved, even if a firewall is present. This vulnerability can be used by intruders to crash vulnerable NT servers.	Customers who are unsure whether they are potentially affected by this vulnerability should check their systems for the following files: ISM.DLL SSINC.DLL HTTPODBC.DLL If any of these files are present, IIS 4.0 is installed and the system is potentially vulnerable. The patch that eliminates this vulnerability is available at: ftp://ftp.microsoft.com/bus/sys/IIS/iis-public/fixes/usa/ext-fix/	IIS Remote Buffer Overflow Vulnerability**	Very High	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has been discussed in the press. Exploiting the flaw requires no special tools or knowledge. The exploit has also been ported to Linux.

²³ Bugtraq, June 4, 1999.

²⁴ Bugtraq, June 7, 1999.

²⁵ eEye Digital Security Team, June 8, 1999.

** IIS Remote Buffer Overflow aka –
eEye – Retina vs. IIS4 Round 2 – The Exploit;
CERT (CA-99.07) – IIS Buffer Overflow;
CIAC (J048)- Malformed HTR Request Vulnerability;
MS (MS99-019) – “Malformed HTR Request” Vulnerability;
IIS – Malformed HTR File Vulnerability.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between June 5 and June 18, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing.** During this period, 39 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
June 16, 1999	Cmailrbof.c	Exploit code for C-Mail SMTP Serer remote buffer overflow that allows malicious attacker to execute arbitrary code remotely.	
June 16, 1999	Hv-cf.pl	Perl script that scans a given list of hosts for ColdFusion security vulnerabilities.	
June 16, 1999	Hv-pop3crack.pl	Perl script that executes dictionary file based brute force attacks on POP3 account passwords.	
June 16, 1999	Iishack.exe	Executable eEye NT4 +IIS4 URL buffer overflow remote exploit program. Use with one of the ncx* files in the eEye.retina.vs.iss4.zip file.	
June 16, 1999	Novell.4.x.http.dos.c	Exploit code for Novell Netware 4.x web server Denial of Service attack.	
June 16, 1999	Pizzathief32.c	Win32 port of exploit code for Microsoft Windows 2000 FTP server PASV vulnerability that allows malicious attacker to hijack your connection and steal the files you attempt to download.	
June 16, 1999	Spike.sh4.zip	Command attack tool that utilizes a wide variety of popular and effective Denial of Service scripts. Features options to launch varying degrees of attacks. And a menu to choose attacks from.	
June 15, 1999	Iis.injector.c	IIS Injector for NT is a custom C port of the eEye NT4+IIS4 URL buffer overflow remote exploit that allows the attacker to select any desired "payload file" for targets.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
June 15, 1999	iis4.htr-2.pl	Perl exploit code port of the eEye NT4+IIS4 Url buffer overflow remote exploit.	
June 14, 1999	Tesoiis.c	Unix port of the eEye NT4+IIS4 URL buffer overflow remote exploit, coded in C.	
June 14, 1999	Wc30b1.zip	Password cracker designed to brute force login/password combinations for web sites that use HTTP-based password authentication.	
June 13, 1999	Net-fizzV0.1.zip	Multithreaded netshare scanner for Windows NT. Reveals hidden shares; command line interface.	
June 13, 1999	Nostrobe.tar.gz	Port scan detection/reporting programs.	
June 12, 1999	Fick-fingerd.gz	Fingerd Denial of Service exploit code.	
June 12, 1999	Gscan.zip	Gscan is a generic banner scanner for windows, class A greps for any banner on any port.	
June 10, 1999	Solaris2.5.su.expect.txt	Sun Solaris 2.5 and earlier contain security hole in the 'su' program that allows scripted brute force attacks on the superuser password without the attacker being logged.	
June 10, 1999	Cgi-check99.2.r	REBOL-based Cgi vulnerability scanner that checks for 70 unique remote CGI security holes.	
June 10, 1999	Cgichk1.51.1.c	CGI scanner v1.51.11 scans remote hosts for over 70 common CGI security holes.	
June 10, 1999	Lamescan-2.DEVEL1990607.tar.gz	Multithreaded portscanner supports scanning domains, Class A, B, C nets, random scan, multithreaded scan, scanning hostnames as they are typed, sending a "user lalala" string to any open port, output to a filename and delaying between each connect() call.	
June 9, 1999	Frootcake.c	Windows NT allows any local user to take advantage of Microsoft's multi-thread code design to bring NT machines to a quick halt. All versions of NT affected.	
June 8, 1999	EEye.retina.vs.iis4.txt	Security hole in Windows NT 4 web servers running IIS allows remote attacker to execute arbitrary code. Detailed exploit description, and four exploit scripts.	
June 8, 1999	EEye.retina.vs.iss4-zip	Complete package of the eEye NT4+IIS\$4 Url buffer overflow remote exploit advisory and code.	
June 8, 1999	iis4.htr.pl	See description for iis4.htr-2.pl.	
June 8, 1999	Iishack.asm	Asm source code for eEye NT4 +IIS4 URL buffer overflow remote exploit Use with one of the ncx* files in the eEye.retina.vs.iss4.zip file.	
June 8, 1999	Msie.activex.filesearch.txt	Security holes in Microsoft internet Explorer 3.x, 4.x, 5.x and ActiveX allows malicious remote attacker to search user hard drives for files and possibly more. Exploit code included.	
June 8, 1999	Ncx.exe	Hacked netcat-based trojan used to exploit the eEye NT4+IIS4 Url remote buffer overflow – gain remote control over NT servers with this backdoor.	
June 8, 1999	Retina.vs.iis4-round2-the.exploit.txt	Details about how and why the eEye NT4+IIS4 URL buffer overflow remote exploit hole was exploited and released.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
June 7, 1999	Atecheck.c	WinGate scanner checks for remote insecure WinGate proxy servers.	
June 7, 1999	Gammaprog-config.tgz	Bruteforce password cracker for web based e-mail address and regular POP3 account.	
June 7, 1999	Gin.c	Spoofs ICMP packets containing +++ATHO which will cause some modems to disconnect.	
June 7, 1999	Sockcheck.c	Socks proxy scanner checks for remote insecure Socks proxy servers.	
June 6, 1999	Netscape viewtrack.txt	Bug in Netscape Communicator 4.x allows attacker to "sniff" URLs from another window using JavaScript and the "view-source:" protocol.	
June 6, 1999	Netscape.datatrack.txt	Bug in Netscape Communicator 4.x allows attacker to "sniff" URLs from another window using JavaScript and the "data:" protocol.	
June 6, 1999	Omnihttpd.webserver.txt	Security vulnerability in OmniHTTPd Web Servers allows remote attacker to execute Denial of Service attacks by filling the server's hard drive.	
June 6, 1999	Redhat.6.0.ptx.permissions.txt	RedHat 6.0 contains a /dev/pts permissions bug that can be exploited by local users if other users are using X-windows. Denial of service attacks.	
June 5, 1999	Apike.sh.zip	Command line attack tool that utilizes a wide variety of Denial of Service scripts. Features options to launch varying degrees of attacks, and a menu to choose attacks from.	
June 5, 1999	Kuang2pSender v0.21 & pSender FULL v0.34	Suite of password retrieving programs that can be used to find all passwords locally, or, with the pSender and tLoader trojan wrappers, to have remote passwords emailed to a specific address.	
June 5, 1999	Macos.x.server.cgi.txt	Process-based Denial of Service vulnerability exists in MacOS X Server running Apache that allows remote attacker to easily kill the web server via looped HTTP requests.	
June 5, 1999	Opentear.c	Denial of Service exploit code that sends lots of fragmented UDP packets. Crashes OpenBSD 2.3/2.4.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

1. Worms that actively exploit IIS vulnerability and seek out other vulnerable hosts have been or are currently being developed.
2. Virus and worm attacks on information systems has increased significantly this year.
3. Ftp and frag attack combinations have escalated recently.
4. Hackers are currently testing methods to defeat detection systems. These include experimentation with timing thresholds and scanning methodologies.
5. Denial of Service attacks are becoming of increasing concern.
6. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.

Viruses

ExploreZip.exe or ZippedFiles.exe – A new e-mail computer infection known as Worm.explore.zip has swept the Internet, showing up quickly in thousands of computers around the world and leading to the shutdown of some corporate e-mail systems. This was first discovered in Israel and is now spreading worldwide. It is a trojan worm with a damaging payload that attacks Windows 95/98/NT systems. Once activated, it uses MAPI compliant email systems, such as Microsoft Outlook, Outlook Express, and Exchange to send itself out to other users by replying to incoming e-mail messages and attaching itself to the reply. The worm will also reduce to zero the file size of any file with the extension .c, .h, .cpp, .asm, .doc, .ppt, or .xls that it finds on the infected system's hard-drive or on any mapped drives, rendering the files unusable. The risk of re-infection is very high. Unless every single machine in a networked environment has been scanned and cleaned, there is potential for the network to become re-infected and for additional data to be lost.

The body of the e-mail message may also contain the following text:

Hi [Recipient Name]!
I received your email and I shall send you a
reply ASAP.
Till then, take a look at the attached zipped
docs.
Bye

Anyone who receives an e-mail similar to the one above, should not extract and execute the attached program. Receipt of the message should be reported to local computer security personnel.

Subseven (June 14, 1999) – A malicious trojan identified is being distributed under various names via newsgroups and e-mail. When executed, Subseven.backdoor.C creates a special hidden link allowing the hacker to view and control your computer system remotely. This permits the hacker to access files and personal information on your local system or company network.

Deep Throat (June 14, 1999) – The current Deep Throat 3.0 is a buggy release. It offers many more features and a better client for the hacker. It's keylogger uses port 999 TCP by default and its FTP server uses 41 TCP. The port redirection, a new feature to Deep Throat is defaulted for making the hacker's IRC IP number the one of the trojan's.

Netsphere (May 31, 1999) – This is another Trojan used as a "hack" tool. This program might be even more advanced than NetBus x.x. The server part is designed to make your system vulnerable to hackers.